SHUSTOKE C OF E PRIMARY SCHOOL

‘Living life in all its fullness.’ John 10:10

At Shustoke, all are encouraged to flourish and let their light shine. Passionate staff guide and support children to become compassionate, respectful, forgiving and confident individuals equipped to persevere when faced with challenges and to serve their community as Jesus taught us. Like a tree planted by streams of water, Children grow strong in wisdom. They explore talents, interests, and spirituality through opportunities to live life in all its fullness. Through our shared values, loving relationships are nurtured, and doors are opened to a future filled with hope, joy, and peace. Together, we all thrive.

Online Safety and ICT Acceptable Use Policy

Approval Date	**January 2025**
Review Date	**January 2026**
Governors’ Sub-Committee	**Curriculum and Standards**
Statutory Policy	**No**

1. Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter and Snapchat
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting, Video sharing and Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Shustoke C of E Primary School, we understand the responsibility to educate our children on online safety issues including safeguarding, radicalisation, extremism and protecting their personal data; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of personal information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners. Schools must be mindful to protect personal data to comply with GDPR regulations as set out under the Data Protection Act 2018.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement for all staff, governors, regular visitors and children are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, whiteboards, google forms, digital video equipment etc),

and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

2. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request and GDPR regulations more generally under the Data Protection Act 2018 or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

3. Breaches

A breach or suspected breach of policy by a school employee, contractor or child may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Breaches to personal data must be reported to the Information Commissioner's Office (ICO) within 72 hours (reference Data Protection Policy).

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings. The ICO's powers to issue monetary penalties came into force on 25 May 2018, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £18 million for serious breaches of the Data Protection Act.

The ICO has both investigative and corrective powers including but exclusive to:

- Carry out investigations – data protection audits;
- Access all personal data and any premises and processing equipment from controller/processor;

- Issue to warnings to controller/processor if intended processing operations likely to infringe GDPR;
- Issue reprimands where processing has infringed GDPR;
- Order processing operations are brought into compliance;
- Order rectification or erasure and impose a fine or withdraw certification;
- Limit or ban processing temporarily or indefinitely.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Mrs Clare Brighton (Office Manager and Data Protection) Miss Michele Wall, (Headteacher)

4. Staff Professional Responsibilities

When using any form of ICT, including the Internet, in school and outside school, for your own protection we advise that you:

- Ensure all electronic communication with children, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook, Twitter and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to children, parents, carers and others.
- Do not disclose any passwords and ensure that personal data is kept secure and used appropriately.
- Only take images of children and/ or staff for professional purposes, in accordance with school policy (Data Protection Policy) and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, both in school and outside school, will not bring the School or your professional role into disrepute.
- You have a duty to report any online safety incident which may impact on you, your professionalism or the School.

Computer Viruses

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment, turn the device off and place the following notice on the computer "Not in use". Thereafter contact then Office Manager immediately
- The School has virus software installed on school devices.

5. Data Security

Data Protection: key responsibilities for School Heads and Governors

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used. This aligns to policy directives as set out in the School's Data Protection Policy.
- Anyone sending a confidential or sensitive email or fax should notify the recipient before it is sent.

6. Relevant Responsible Persons

The Computing Lead is Amy Turner and the ICT technician is Mike Daniels.

- They will advise school staff on appropriate use of school technology.

7. Email

7.1 Managing email

- Where appropriate and relevant, the school gives all staff, children and governors their own email account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- The school can provide access to school email accounts for others as and when required – for educational purposes.
- Staff & governors should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email

histories can be traced. The school email account should be the account that is used for all school business.

- Under no circumstances should staff contact children, parents/carers or conduct any school business using personal email addresses. Nor should staff contact children and parents/carers using their school issued email address.
- The school uses the school website to send/receive email communication with parents/carers.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails of a confidential nature, e.g. matters pertaining to safeguarding and child protection, are advised to cc. the Headteacher, or one of the deputy DSLs (Emma Davison, Catherine Brown, Alison Harrison or Julie Babbs)
- Children may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000/Data Protection 2018. You must therefore actively manage your email account as follows:
  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives
  - Composition of emails must be, at all times, professional in tone and manner.

7.2 Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information
- Use only the School's email account s(shustokeparents@welearn365.com or shustokelearning@welearn365.com) when communicating with parents/carers. Staff are advised not to use their own school email account.
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily.

7.3 Receiving emails

- Check your email regularly.
- Never open attachments from an untrusted source.
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of emails is not allowed.

7.4 Emailing Personal or Confidential Information

Where your conclusion is that email must be used to transmit such data:

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

8. Online Safety (formerly E-Safety)

Online Safety - Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Whole School ICT coordinator (Online Safety Coordinator) in this school is Mrs Amy Turner. All members of the school community have been made aware of who holds this post. It is the role of the Computing Lead to keep abreast of current issues and guidance.

Senior Leadership and governors are updated by the Computing Lead and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and children, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, data protection, home–school agreements, and behaviour (including the anti-bullying) policy and PHSE.

Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. It is essential for online safety guidance to be given to the children on a regular and meaningful basis. Online Safety is embedded within our curriculum and we continually look for new opportunities to promote online safety.

- The school has a framework for teaching online safety in Computing lessons across the school
- Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of Computing and PSHE
- Children are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button.

Online safety when Remote Learning

The aim is to teach the curriculum in a way so that learning from home replicates the school experience as best it can in remote circumstances. All other school policies will be followed and replicated, whether children are learning from school or from home. We accept there may be times when this cannot be adhered to completely due to for example issues with technology (school and/or home) or by acknowledging that all children's' home circumstances are different – some for example may struggle more with keeping up with work set via home learning. When staff are required to work from home in order to deliver education, Shustoke C of E Primary School shall:

- Provide staff with a secure, school registered device to work from.
- Ensure staff are briefed and familiar with the school's remote working policy.
- Ensure all staff are up to date with data protection training.

When implementing a platform where students are required to engage in online activities, Shustoke C of E Primary School will:

- Ensure parents are informed of the type of work children are being asked to do.
- Provide information on who is likely to engage with pupils online in order to deliver online teaching.
- Share information and guidance with parents to ensure they are able to effectively monitor their children's safety online.
- Review settings to ensure they are set to the most secure and practical format that is possible.
- Review privacy settings of all platforms used for online teaching to ensure children are not placed at risk.
- If uploading information to an open cloud-based system, we will ensure no personal information that identifies individuals is included.
- Take all reasonable steps to ensure that risks of harm to children through inappropriate access via online portals are reduced as far as possible.
- Continuously liaise with our safeguarding team to ensure we are following all relevant safeguarding guidance.

Online Safety Skills Development for Staff

- Our staff receive regular information and training on online safety and how they can promote the 'Stay Safe' online messages in the form of staff briefings and INSET training.
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School Online Safety Messages

- We endeavour to embed online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The online safety policy will be introduced children at the start of each school year and an acceptable use agreement signed by Parent/ Carer.
- Online Safety posters will be prominently displayed.
- The key online safety advice will be promoted widely through school displays, newsletters,

class activities and so on.

- Online Safety key messages and information will be freely available to all stakeholders via the School's website. This will be actively promoted at all times.

9. Incident Reporting, Online Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or Online Safety Coordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the senior ICT technician.

Online Safety Incident Form

Keeping a record of online safety incidents can identify trends or specific concerns. A record of incidents is kept on CPOMS. ICTDS monitor and filter incidents on line. A call will be made to school from the service and this is followed up with an email which is retained on the school system. Any safeguarding issues arising from online safety incidents must be passed to the Senior DSL

Misuse and Infringements

Complaints

Complaints and/ or issues relating to online safety should be made to the Headteacher.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Michele Wall (Headteacher) and Emma Davison (Deputy Headteacher). Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct by following the appropriate conditions as set out within the School's Code of Conduct.

10. Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- The school provides children with supervised access to Internet resources (where reasonable) through the school's fixed and Wi-Fi internet connectivity.
- Staff will preview any recommended sites, online services, software and apps before use.
- Searching for images through open search engines is discouraged when working with children.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Do not reveal names of colleagues, children, others or any other confidential information acquired through your job on any social networking site or other online application.
- On-line gambling or gaming is not allowed.
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Shustoke C of E Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and children are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Computing Lead, Office Manager or teacher as appropriate..
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the senior ICT technician.
- If there are any issues related to viruses, the ICT technician should be informed.

11. Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our children to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Where relevant, the school endeavours to deny access to social networking and online games websites to childfren within school.

- All students are advised to be cautious about the information given by others on such

websites, for example users not being who they say they are.

- Through external agencies such as Loudmouth Theatre group, children are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Children are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)..
- Children are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Our children are asked to report any incidents of Cyberbullying to the school..
- Services such as Facebook, Instagram and Snapchat have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

12. Parental Involvement

It is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website) to comply with GDPR – Data Protection Act 2018.

- The school disseminates information to parents relating to online safety where appropriate.

13. Passwords and Password Security

Passwords

- Always use your own personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
- Never tell a child or colleague your password.
- If you aware of a breach of security with your password or account inform the office manager immediately.
- Passwords must contain a minimum of six characters and be difficult to guess.
- User ID and passwords for staff and students who have left the school are removed from the system within one day of leaving.

If you think your password may have been compromised or someone else has become aware of your password report this to the Office Manager.

Password Security
Password security is essential for staff, particularly as they are able to access and use personal data. Staff are expected to have secure passwords which are not shared with anyone.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety and ICT Acceptable Use Policy.
- Users are provided with an individual network, email, and Management Information System log-in username. They are also expected to use a personal password and keep it private.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic screen lock for the school network is 30 minutes.

14. GDPR – Data Protection Compliance

- Ensure that any school information (personal data) accessed from your own PC is kept secure and is not removed from the school network.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal or sensitive information you disclose or share with others and only share personal or sensitive information that is absolutely necessary – remember, do they require this information and in what format?
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal or sensitive information contained in documents you email, fax, copy, scan or print. This is particularly important when shared copiers (multifunction print, fax, scan and copiers) are used.
- Only download personal data from systems if expressly authorised to do so
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of securely

Storing/Transferring Personal or Sensitive Information Using Removable Media

- Encrypted removable storage devices are the only allowed storage device permitted to access the school's network.
- Securely dispose of removable media that may hold personal data.

15. Remote Desktop Access

- You are responsible for all activity via your remote desktop access facility.
- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all logon IDs confidential and do not disclose them to anyone.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect school information and data at all times. Take particular care when access is from a non-school environment.

16. Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. This complies with GDPR regulations (Data Protection Act 2018). Please refer to the School's Data Protection Policy.

- With the written consent of parents/carers (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Parents/carers must sign the school's GDPR consent form to give their consent (opt in) to the taking of images by staff and students with school equipment. The School in turn will keep an official record of consent given by parents/carers on the School's MIS.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on school/field trips, unless with the express permission of the School's Designated Data Protection Lead or the Headteacher (images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device).
- The School will check the School's records to check which children and staff have permission before any image can be uploaded for publication.

Consent of Adults Who Work at the School

- Consent to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Student's Images

On a child's entry to the school, all parents/carers will be asked to give their consent to use their child's photos as below:

I give permission for my child's photograph to be used within school for display purposes.	YES / NO
I give permission for my child's image to be shared with other children/parents within their class (Such as end of year group photos taken by teacher, photos taken on a school trip or photos taken during class assemblies/ Nativity)	YES / NO
I give permission for my child's image to be used on our school website, including in the weekly newsletter.	YES / NO
I give permission for my child to appear in the media (local newspaper, prospectus), including on their website/social media feed.	YES / NO
I give permission for my child image/film to be used on school social media.	YES / NO
I give permission for my child to be filmed for the purpose of school productions/performances. I understand that this footage will be made available to the parents/carers of other children involved.	YES / NO

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Childrens' full names will not be published alongside their image. Permission will be sought from parents before publishing any pieces of work (such as in the weekly newsletter)

Storage of Images

- Images/ films of children are stored securely on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource.
- Amy Turner (Computing Lead) has the responsibility of deleting the images when they are no longer required, or then the student has left the school.

17. School ICT Equipment & Mobile ICT Equipment

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.
- It is recommended that the school logs ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device.
- All school issued laptops are encrypted.
  It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network, apart from internet access which must be approved by the senior ICT technician.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the Assistant Headteacher responsible for e-learning. ICT technicians are responsible for:
  - maintaining control of the allocation and transfer back into school ready for reissue.
  - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey in line with the School's Data Protection Policy.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the ICT technician or WES ICT.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if sup

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Never use a hand-held mobile phone whilst driving a vehicle.

18. Social Media, including Facebook and Twitter

Facebook, Instagram, Twitter and other forms of social media are increasingly becoming an important part of our daily lives, however Shustoke C of E Primary School do not currently use these platforms.

19. Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act and The Data Protection Act 2018, namely GDPR (General Data Protection Regulations).
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply

delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

20. Writing and Reviewing this Policy

Governors

- Governors have been made aware of the contents of this policy and will review as part of the policy review schedule.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

21. Current Legislation

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.legislation.gov.uk/ukpga/2018/12/enacted

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.legislation.gov.uk/ukpga/2000/23/contents

Human Rights Act 1998

http://www.legislation.gov.uk/ukpga/1998/42/contents

Other Acts Relating to E-Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
http://www.legislation.gov.uk/ukpga/2006/1/contents

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
http://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.
http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another person's password to access files).
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program.

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences. http://www.legislation.gov.uk/ukpga/1990/18/section/1
http://www.legislation.gov.uk/ukpga/1990/18/section/2
http://www.legislation.gov.uk/ukpga/1990/18/section/3
http://www.legislation.gov.uk/ukpga/1990/18/section/3ZA
http://www.legislation.gov.uk/ukpga/1990/18/section/3A

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.
http://www.legislation.gov.uk/ukpga/1988/27/section/1

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. http://www.legislation.gov.uk/ukpga/1986/64/part/III

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.
http://www.legislation.gov.uk/ukpga/1978/37/section/1

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
http://www.legislation.gov.uk/ukpga/1964/74/contents

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

http://www.legislation.gov.uk/ukpga/1997/40/contents

Acts Relating to the Protection of Personal Data

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/enacted

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & CounterExtremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrensservices